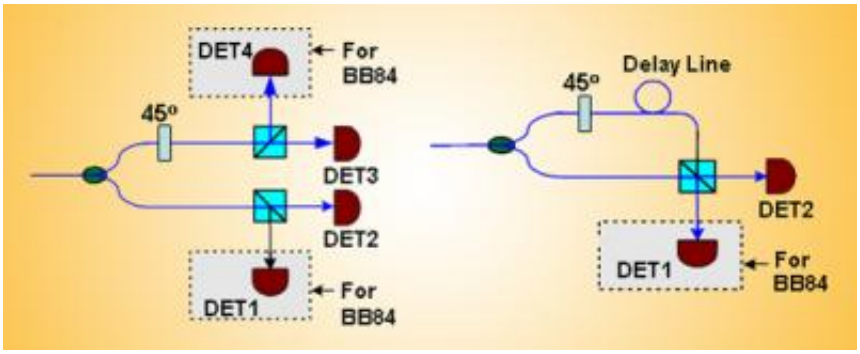
# Two for One: New Design Enables More Cost-Effective Quantum Key Distribution

May 29 2008




A highly simplified schematic of a recipient's detectors in a quantum cryptography setup. Conventional cryptography setups (left) require at least two detectors, and the most common setup, known as BB84, requires four. By adding an optical component that delays the travel of photons to the detector, the number of required detectors is cut in half. Credit: NIST

Researchers at the National Institute of Standards and Technology have demonstrated a simpler and potentially lower-cost method for distributing strings of digits, or “keys,” for use in quantum cryptography, the most secure method of transmitting data. The new “quantum key distribution” (QKD) method, outlined in an upcoming paper, minimizes the required number of detectors, by far the most costly components in quantum cryptography.

Although this minimum-detector arrangement cuts transmission rates by half, the NIST system still works at broadband speeds, allowing, for

example, real-time quantum encryption and decryption of webcam-quality video streams over an experimental quantum network.

In quantum cryptography, a recipient (named Bob) needs to measure a sequence of photons, or particles of light that are transmitted by a sender (named Alice). These photons have information encoded in their polarization, or direction of their electric field. In the most common polarization-based protocol, known as BB84, Bob uses four single-photon detectors, costing approximately $5,000-$20,000 each.

One pair of detectors records photons with horizontal and vertical polarization, which could indicate 0 and 1 respectively. The other pair detects photons with “diagonal”, or +/- 45 degree, polarization in which the “northeast” and “northwest” directions alternatively denote 0 and 1.

In the new method, the researchers, led by NIST’s Xiao Tang, designed an optical component to make the diagonally polarized photons rotate by a further 45 degrees and arrive at the same detector but later, and into a separate “time bin”, than the horizontal/vertical polarized ones.

Therefore, one pair of detectors can be used to record information from both kinds of polarized photons in succession, reducing the required number of detectors from four to two. In another protocol, called B92, the researchers reduced the required number of detectors from two to one. And in work performed since their new paper, the researchers further developed their approach so that the popular BB84 method now only requires one detector instead of four.

Although in theory quantum cryptography can transmit absolutely secure keys guaranteed by fundamental physical principles (measuring them will disturb their values and make an eavesdropper instantly known), the imperfect properties of photon detectors may undermine system security in practice.

For example, photon detectors have an intrinsic problem known as “dead time,” in which a detector is out of commission for a short time after it records a photon, causing it to miss the bit of data that immediately follows; this could result in non-random (and therefore more predictable) bit patterns in which 0s alternate with 1s. Furthermore, inevitable performance differences between detector pairs can also cause them to record less random sequences of digits. The new design avoids these issues and maintains the security of quantum-key-distribution systems in practical applications.

Citation: L. Ma, T. Chang, A. Mink, O. Slattery, B. Hershman and X. Tang. Experimental demonstration of a detection-time-bin-shift polarization encoding quantum key distribution system. *IEEE Communications Letters* Vol. 12, No. 6, June 2008. In press.

Source: National Institute of Standards and Technology